REMARKS/ARGUMENTS

Favorable reconsideration of this application, in light of the present amendments and following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending; Claims 1, 9, 11, 19, 21, and 22 having been amended. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, on page 30, line 5 to page 32, line 18, and Figs. 7A-7B, and 8A-8C.

In the outstanding Office Action, Claims 1-5, 9-15, and 19-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography," Second Edition) in view of Bo Lin et al. (GB 2345229A, hereafter "Lin"); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter "Kocher"); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter "Kaminaga").

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection. Amended Claim 1 recites, *inter alia*,

> a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group including a triple-DES encryption process, and by mixing processing sequences of encryption processing units of the plurality of groups with each other so that performance of at least one process from one of the groups is performed at a time between processes from another one of the groups and under a condition in which the processing sequence of the encryption processing units within each set group is fixed;...
>
> wherein said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption

> processing sequence in at least one of said groups of divisions, and set the number of dummy single-DES processes to be a multiple of 3.

Applicants respectfully submit that Schneier and Lin fail to disclose or suggest these features of Claim 1.

Schneier is directed to a description of the Data Encryption Standard (DES). DES includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier). Schneier also describes Triple Encryption in which a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier).

The Office Action takes the position that Schneier discloses the claimed "dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units" because it describes Triple Encryption and Triple-DES Cipher Block Chaining (CBC) encryption and DES encryption has 16 rounds. (See Office Action at page 3). Therefore, it appears that the Office Action is taking the position that a triple encryption process (either triple DES or CBC) corresponds to the claimed "plurality of groups" and the 16 rounds corresponds to the claimed "one or more encryption processing units." In other words, the Office Action is interpreting each DES process within a triple DES process to be one of the "groups" in the claimed "plurality of groups." The Office Action also takes the position that Schneier discloses "mixing processing sequences" where it describes Triple Encryption and Triple-DES Cipher Block Chaining (CBC). (See Office Action at pages 3-4). In other words, the Office Action interprets the "mixing" of the groups in Schneier to be the existence of a Triple-DES process because it has multiple DES processes.

However, Schneier fails to disclose or suggest that ***each of the plurality of groups includes a triple-DES encryption process*** and mixing processing sequences of encryption

processing units of the plurality of groups with each other so that performance of at least one process from one of the groups is performed at a time between processes from another one of the groups, as defined by amended Claim 1. In other words, Schneier discloses standard encryption processes such as DES, Triple-DES, and CBC. However, Schneier does not disclose mixing performance of processes from one group that includes a triple-DES process with another group that also includes a triple-DES process, as defined in Claim 1.

Therefore, Schneier fails to disclose or suggest "a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group including a triple-DES encryption process, and by mixing processing sequences of encryption processing units of the plurality of groups with each other so that performance of at least one process from one of the groups is performed at a time between processes from another one of the groups and under a condition in which the processing sequence of the encryption processing units within each set group is fixed," as defined by amended Claim 1.

Lin has been considered but fails to remedy this deficiency of Schneier.

Thus, Applicants respectfully submit that amended Claim 1 (and all associated dependent claims) patentably distinguish over Schneier and Lin, either alone or in proper combination.

Amended independent Claims 11 and 21 recite features similar to those of amended Claim 1. Thus, Applicants respectfully submit that amended Claims 11 and 21 (and all associated dependent claims) patentably distinguish over Schneier and Lin, either alone or in proper combination.

Additionally, with regard to Claim 1, the Office Action admits that Schneier fails to disclose or suggest "said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing

sequence in at least one of said groups of divisions, and set the number of dummy single-DES processes to be a multiple of 3 corresponding to the triple DES encryption process." (See Office Action, for example, at page 4).

The Office Action relies on Lin to remedy this deficiency of Schneier. Lin describes inserting dummy S-block lookups into a real DES process (see page 11, lines 10-13). However, Lin does not describe making an ***entire*** single-DES process as a dummy itself. The Office Action takes the position that based on Lin's description of dummy lookups it would be obvious to set the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to triple DES because each number of single-DES is set to 1. (See Office Action at page 5). However, as discussed above, Lin describes inserting dummy look-ups into a DES process. Therefore, multiplying a dummy look-up process by 3 does would only achieve 3 dummy look-up processes, which is not the same as 3 dummy DES processes.

Therefore, Lin fails to disclose or suggest "said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups of divisions, and set the number of dummy single-DES processes to be a multiple of 3," as defined by Claim 1.

Claims 9, 11, 19, 21, and 22 recite features similar to the foregoing feature discussed above for Claim 1. Thus, Applicants respectfully submit that Claims 1, 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier and Lin, either alone or in proper combination, for at least the foregoing reasons.

Furthermore, amended Claim 9 recites, *inter alia*,

> a control section configured to set a mixed encryption processing sequence by dividing the original encryption processing sequence, which includes a triple DES encryption process, into one or more encryption processing units, by adding a dummy encryption processing unit that performs a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence and that

> corresponds to said encryption processing unit, and by performing a mixing of processing sequences of the original encryption processing units included in the original encryption processing sequence and said dummy encryption processing units so that performance of at least one process from the original encryption processing sequence is performed at a time between processes from the dummy encryption process.

As discussed above, Schneier discloses standard encryption processes such as DES, Triple-DES, and CBC. However, Schneier fails to disclose or suggest that performance of at least one process from the original encryption processing sequence that includes a triple-DES process is performed at a time between processes from a dummy encryption process, as defined by amended Claim 9.

Lin has been considered, but fails to remedy this deficiency of Schneier with regard to Claim 9. Thus, Applicants respectfully submit that amended Claim 9 (and all associated dependent claims) patentably distinguish over Schneier and Lin, either alone or in proper combination.

Amended Claims 19 and 22 recite features similar to those of amended Claim 9. Thus, Applicants respectfully submit that amended Claim 19 and 22 (and all associated dependent claims) patentably distinguish over Schneier and Lin, either alone or in proper combination.

Kocher and Kaminaga have been considered but fail to remedy the deficiencies of Schneier and Lin with regard to Claims 1, 9, 11, 19, 21, and 22 as discussed above. Thus, Applicants respectfully submit that Claims 1, 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\SG\24's\247305US\247305US-AM-DUE-6-18-08.DOC